

Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation

Wei Zhang · Dao-Wen Qiu · Xiang-Fu Zou

the date of receipt and acceptance should be inserted later

Abstract Recently, a broadcasting multiple blind signature scheme based on quantum teleportation has been proposed for the first time. It is claimed to have unconditional security and properties of quantum multiple signature and quantum blind signature. In this paper, we analyze the security of the protocol and show that each signatory can learn the signed message by a single particle measurement and the signed message can be modified at random by any attacker according to the scheme. Furthermore, there are some participant attacks and external attacks existing in the scheme. Finally we present an improved scheme and show that it can resist all of the mentioned attacks. Additionally, the secret keys can be used again and again, making it more efficient and practical.

Keywords Security analysis · quantum broadcasting multiple blind signature · quantum teleportation

W. Zhang · D.-W. Qiu
Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China
The Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China
E-mail: issqdw@mail.sysu.edu.cn

W. Zhang
Department of Mathematics, Qiannan Normal College for Nationalities, Duyun 558000, China

X.-F. Zou
School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China

1 Introduction

Quantum signature is the counterpart in the quantum world of classical digital signature. Most classical digital signature schemes are based on public key cryptography which can be broken by Shor's algorithm [1]. Quantum signature, which is based on the laws of quantum physics, can provide us unconditional security. Many different quantum signature models are proposed for different application demands, such as arbitrated quantum signature [2, 3, 4, 5, 6, 7], quantum proxy signature [8, 9, 10, 11], quantum group signature [12, 13, 14, 15], quantum blind signature [16, 17, 18] and quantum multiple signature [19, 20].

A secure quantum signature scheme should satisfy the following two basic requirements: (1) No forgery. Specifically, the signature cannot be forged by any illegal signatory. (2) No disavowal. The signatory cannot disavow his signature and the receiver cannot disavow his receiving it. Furthermore, the receiver cannot disavow the integrity of the signature [4].

As quantum cryptography has developed, many cryptanalysis of existing protocols have been presented [21, 22, 23, 24, 25, 26, 27]. Some effective attack strategies also have been proposed to eavesdrop in the existing quantum cryptography protocols [28], such as intercept-resend attacks [29], entanglement swapping attacks [30, 31, 32], teleportation attacks [33, 34], dense-coding attacks [35, 36, 37], channel-loss attacks [38, 39], denial-of-service attacks [40, 41], correlation-extractability attacks [42, 43, 44], Trojan horse attacks [45, 46, 47, 48], participant attacks [49] and collaborate attacks [50]. Understanding these attacks is very important for designing quantum signature schemes with higher security. It also advances the research in quantum signature. Zou and Qiu [4] analyzed the arbitrated quantum signatures based on GHZ states and Bell states, finding that the receiver Bob can successfully reject the signature by disavowing its integrity. Then they proposed a new scheme by using a public board to fix this security loophole in which the entanglement was not needed any more.

Gao et al. [21] gave a perfect cryptanalysis on existing arbitrated quantum signature. They found that the signature can be forged by the receiver at will in almost all the existing AQS schemes and the sender can disavow the signature just by an intercept-resend method. Due to the existence of serious loopholes, it is imperative to reexamine the security of other quantum signature protocols.

Recently, a broadcasting multiple blind quantum signature scheme based on quantum teleportation has been proposed in Ref. [51]. It is said to have the properties of both quantum multiple signature and quantum blind signature. Here we show that it is not a real blind signature because the signatory can get the content of the signed message. In addition, the signed message can be modified at random by any attacker. Moreover, there are some participant attacks and external attacks existing in the scheme. For instance, the message sender Alice can impersonate U_i successfully as she can get the content of the signature and U_i 's secret key K_{CU_i} . Moreover, Alice can sign arbitrary message at will. The signature collector Charlie can counterfeit the signature

optionally. With respect to the external attacks, the eavesdropper Eve can forge U_i 's signature at will without knowing the secret key K_{CU_i} .

All the attack strategies are described in detail and finally we present an improved scheme which can resist all the mentioned attacks. Meanwhile, since all the secret keys can be reused, it may greatly increase the scheme's efficiency and make it more practical.

The rest of this paper is organized as follows. First, in Section 2 we review the original protocol briefly. In Section 3 we present the security analysis of the original protocol and describe the attack strategies in detail. In Section 4 we present an improved scheme and analyze its security by showing that the improved one can resist all the attacks mentioned above and that the keys can be used again and again. In Section 5 a short conclusion is given and an issue worthy on further research is proposed.

2 Review of the original protocol [51]

The protocol involves the following four characters: (1) Alice is the message sender. (2) U_i is the i -th member of broadcasting multiple signatory. (3) Charlie is the signature collector. (4) Bob is the receiver and the verifier of the broadcasting multiple blind signature.

The scheme is composed of three parts: the initial phase, the individual blind signature generation and verification phase, and the combined multiple blind signature verification phase.

In this scheme, Alice sends t copies of n -bit classical message m to t signatories U_i ($i = 1, 2, \dots, t$) respectively, then U_i signs the message m to get the blind signature S_i and sends S_i to Charlie. Charlie collects and verifies these blind signatures, then he constructs a multiple signature and sends it to Bob. Finally, Bob verifies the multiple signature by confirming the message.

(1) Initial phase

(1.1) Alice transforms the classical message m into n -bit as

$$\begin{aligned} m &= m(1)||m(2)||\dots||m(j)||\dots||m(n), \\ m(j) &= 0 \quad \text{or} \quad m(j) = 1, \\ j &= 1, 2, \dots, n. \end{aligned} \tag{1}$$

(1.2) Quantum key distribution

Alice shares a secret key K_{AB} with Bob, a secret key K_{AC} with Charlie, and secret keys K_{AU_i} ($i = 1, 2, \dots, t$) with each signatory U_i , respectively. Bob shares a secret key K_{BC} with Charlie, Charlie shares secret keys K_{CU_i} ($i = 1, 2, \dots, t$) with each signatory U_i respectively. To obtain unconditional security, all these keys are distributed via QKD protocols.

(1.3) Alice sends $E_{K_{AB}}^C(m)$ to Bob

Here E^C means classical one-time pad algorithm,

$$E_{K_{AB}}^C(m) = K_{AB} \oplus m. \tag{2}$$

E_K^Q in the later means quantum one-time pad

$$E_K^Q(|P\rangle) = \bigotimes_{i=1}^n \sigma_x^{k_{2i-1}} \sigma_z^{k_{2i}} |P_i\rangle, \quad (3)$$

K is a secret key with $|K| = 2n$, K_i is the K 's i -bit. $|P\rangle$ is an n -bit quantum message, $|P_i\rangle$ is its i -bit. σ_x and σ_z are two Pauli operators.

(2) The individual blind signature generation and verification phase

In this phase, we pick one of the signatory U_i as the representative who signs the message.

(2.1) Message transformation

Assume that Alice is to send the message m . She prepares n -qubit state $|\psi(m)\rangle_M$ as

$$|\psi(m)\rangle_M = \bigotimes_{j=1}^n |\psi(j)\rangle_M, \quad (4)$$

where

$$|\psi(j)\rangle_M = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M) & \text{if } m(j) = 1 \\ \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M) & \text{if } m(j) = 0. \end{cases} \quad (5)$$

(2.2) Quantum channel setup

Alice prepares n EPR pairs. Each pair is denoted as

$$|a(j)\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC} + |11\rangle_{AC}), j = 1, 2, 3, \dots, n+l. \quad (6)$$

(2.3) Signature Phase

(2.3.1) Alice picks up her n EPR particles denoted as $\{|\varphi(N)\rangle_A\}$, i.e.

$$\{|\varphi(N)\rangle_A\} = \{|\varphi(1)\rangle_A, |\varphi(2)\rangle_A, \dots, |\varphi(j)\rangle_A, \dots, |\varphi(n)\rangle_A\}, \quad (7)$$

and the other n EPR particles denoted as $\{|\varphi(N)\rangle_C\}$, i.e.

$$\{|\varphi(N)\rangle_C\} = \{|\varphi(1)\rangle_C, |\varphi(2)\rangle_C, \dots, |\varphi(j)\rangle_C, \dots, |\varphi(n)\rangle_C\}. \quad (8)$$

(2.3.2) To distinguish each signatory, Alice creates a unique serial number which is denoted as SN attaching to $\{|\varphi(N)\rangle_A\}$. Since SN is a classical string, Alice transfers it to a quantum state sequence $|SN\rangle$ with the basis $B_Z = \{|0\rangle, |1\rangle\}$. Then she sends $E_{KAU_i}^Q(|\psi(N)\rangle_{MA}, |SN\rangle)$ to U_i . Here

$$|\psi\rangle_{MA} = \bigotimes_{j=1}^n |\psi(j)\rangle_M \otimes |\varphi(j)\rangle_A. \quad (9)$$

After that, Alice sends $E_{KAC}^Q(\{|\varphi(N)\rangle_C\}, |SN\rangle)$ to Charlie.

(2.3.3) U_i decrypts $E_{KAU_i}^Q(|\psi\rangle_{MA}, |SN\rangle)$ to get $|\psi\rangle_{MA}$ and $|SN\rangle$, then he performs Bell-basis measurement to get the outcomes $\{\beta_{MA}(j)|j = 1, 2, \dots, n\}$.

Each $\beta_{MA}(j) = \beta_{kl}(k, l \in \{0, 1\})$ is expressed by 2-bit string kl according to $|\beta_{kl}\rangle \mapsto kl$. Then he gets S_i as

$$S_i = \beta_{MA}(1) \parallel \beta_{MA}(2) \parallel \cdots \parallel \beta_{MA}(j) \parallel \cdots \parallel \beta_{MA}(n). \quad (10)$$

(2.3.4) U_i sends $E_{K_{CU_i}}^C(S_i, SN)$ to Charlie.

(2.4) Verification Phase

(2.4.1) Charlie decrypts $E_{K_{CU_i}}^C(S_i, SN)$ to get the signature S_i and SN .

(2.4.2) According to S_i , SN and quantum teleportation, Charlie performs one of the corresponding reverse transformation (I, X, Y, Z) on each particle $|\varphi(j)\rangle_C$ in his hand to get $|\psi'(j)\rangle_C$. He obtains $|\psi'(m)\rangle_C$ as

$$|\psi'(m)\rangle_C = \bigotimes_{j=1}^n |\psi'(j)\rangle_C. \quad (11)$$

(2.4.3) Charlie gets m' by measuring each $|\psi'(j)\rangle$ in the basis of $\{\frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M)\}$. Then he sends $E_{K_{BC}}^C(m')$ to Bob.

(2.4.4) Bob decrypts $E_{K_{BC}}^C(m')$, $E_{K_{AB}}^C(m)$ by the secret keys K_{BC} and K_{AB} respectively and compares m with m' . If they are the same, S_i is accepted. Otherwise, it is rejected.

(3) The combined multiple signature generation and verification phase

(3.1) Charlie collects all individual signatures to generate the multiple signature $S = \{S_i | i = 1, 2, \dots, t\}$ and generates the message $\{m'_i | i = 1, 2, \dots, t\}$. If m'_i is equal to m'_{i+1} ($i = 1, 2, \dots, t-1$), he confirms the message and sends $E_{K_{BC}}^C(m'_1)$ to Bob. If it is not equal, the process is terminated.

(3.2) After Bob decrypts $E_{K_{BC}}^C(m'_1)$ and $E_{K_{AB}}^C(m)$, he accepts S if m'_1 is equal to m , otherwise he terminates the process.

3 Cryptanalysis of the original protocol

In this section, we point out that there are some security loopholes in the scheme in Ref. [51] and describe the corresponding attack strategies in detail.

3.1 Each U_i can learn the signed message m

The scheme is claimed to have properties of quantum blind signature so that the signatory cannot learn the signed message. Here we show that each signatory U_i can get the message just by a single particle measurement.

Suppose Alice wants to send an n -bit classical message m to get U_i 's signature, according to the scheme, she will transform it into n -qubit state $|\psi(m)\rangle_M$ according to Eq. (4) and Eq. (5). Because $\frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M)$ and $\frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M)$ are orthogonal to each other, they can form an orthonormal basis of the two dimensional Hilbert Space. When U_i gets $K_{AU_i}^Q(|\psi(m)\rangle_{MA})$ from Alice in the

signature phase, he can decrypt it and perform a single particle measurement in the basis of $\{\frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M)\}$ on the first state to get the message m , which has no effect on the following process. From this problem, we can see the original scheme is not a real blind signature scheme.

3.2 Any attacker can modify Message m at random

Here we show the signed message m can be modified at random through the intercept-resend method by any attacker, including participant attackers or external attackers.

In the original scheme, message m and m' are encrypted according to the one-time pad encryption algorithm during their transmission. Any attacker can intercept $E_{K_{AB}}^C(m)$ and resend $E_{K_{AB}}^C(m) \oplus m_0$ to Bob in Step (1.3). According to the scheme, Bob will get $m \oplus m_0$ instead of m , here m_0 is an arbitrary $2n$ -bit random binary string. At the same time, he intercepts $E_{K_{BC}}^C(m')$ and resends $E_{K_{BC}}^C(m') \oplus m_0$ in Step (2.4.3). According to the scheme, $m \oplus m_0$ can pass the following verification process. Because m_0 is arbitrary, m can be modified at random by any attacker through intercept-resend method.

3.3 Alice's attack

To illustrate Alice's attack, here take a 1-bit message $m(j)$ to make a demonstration.

3.3.1 Alice can get the signature

Suppose Alice sends the message $m(j)$ to get U_i 's blind signature $S_i(j)$. From the scheme, we can see that U_i signs $m(j)$ by measuring $|\psi(j)\rangle_{MA}$ in the Bell basis, which is sent from Alice in Step(2.3.3). Alice can get $S_i(j) = \beta_{kl}$ by measuring $|\psi(j)\rangle_{MA}$ on Bell basis and recording the outcome β_{kl} before she sends it to U_i . Instead, Alice sends the two particle state $|\beta_{kl}\rangle_{MA}$ to U_i . Then U_i 's measurement outcome is β_{kl} . Then Alice can get each $S_i(j)$.

3.3.2 Alice can get U_i 's secret key K_{CU_i}

It has been illustrated that Alice can get each $S_i(j)$, then Alice can get U_i 's signature S_i . Alice can intercept $E_{K_{CU_i}}^C(S_i)||SN$ when it is sent from U_i to Charlie in Step (2.3.4). Because Alice knows S_i , she can extract U_i 's secret key K_{CU_i} by adding S_i to $E_{K_{CU_i}}^C(S_i)$ as $K_{CU_i} = S_i \oplus E_{K_{CU_i}}^C(S_i)$. Then she resends $E_{K_{CU_i}}^C(S_i)||SN$ to Charlie. All of these cannot be discovered.

3.3.3 Alice can sign the message at will

We can see that Alice can completely replace the signatory U_i to sign the message. In order to illustrate Alice can sign arbitrary message at will, we will demonstrate the quantum teleportation process of the above protocol as follows:

Suppose that the particle M carry a 1-bit classical information $m(j)$ and the state of particle M are denoted as

$$|\psi(j)\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle_M + d|1\rangle_M), \quad d = \pm 1. \quad (12)$$

The EPR pairs shared between Alice and Charlie are denoted as

$$|a(j)\rangle_{AC} = \frac{1}{\sqrt{2}}(|00\rangle_{AC} + |11\rangle_{AC}). \quad (13)$$

The two states are combined to form a three particle state $|\Phi(j)\rangle$ as

$$\begin{aligned} |\Phi(j)\rangle &= |\psi(j)\rangle_M \otimes |a(j)\rangle_{AC} \\ &= \left(\frac{|0\rangle_M + d|1\rangle_M}{\sqrt{2}} \right) \left(\frac{|00\rangle_{AC} + |11\rangle_{AC}}{\sqrt{2}} \right) \\ &= \frac{1}{2} [|\beta_{00}\rangle_{MA} \left(\frac{|0\rangle_C + d|1\rangle_C}{\sqrt{2}} \right) + |\beta_{01}\rangle_{MA} \left(\frac{|1\rangle_C + d|0\rangle_C}{\sqrt{2}} \right) \\ &\quad + |\beta_{10}\rangle_{MA} \left(\frac{|0\rangle_C - d|1\rangle_C}{\sqrt{2}} \right) + |\beta_{11}\rangle_{MA} \left(\frac{|1\rangle_C - d|0\rangle_C}{\sqrt{2}} \right)], \end{aligned} \quad (14)$$

where

$$|\beta_{00}\rangle_{MA} = \frac{|00\rangle_{MA} + |11\rangle_{MA}}{\sqrt{2}}, \quad (15)$$

$$|\beta_{01}\rangle_{MA} = \frac{|01\rangle_{MA} + |10\rangle_{MA}}{\sqrt{2}}, \quad (16)$$

$$|\beta_{10}\rangle_{MA} = \frac{|00\rangle_{MA} - |11\rangle_{MA}}{\sqrt{2}}, \quad (17)$$

$$\text{and } |\beta_{11}\rangle_{MA} = \frac{|01\rangle_{MA} - |10\rangle_{MA}}{\sqrt{2}}. \quad (18)$$

From Eq. (14), we can see if the measurement outcome is β_{00} , the state of the particle C is just the information state $|\psi(j)\rangle_M$. Then we take operation I on the state of C . If the measurement outcome is β_{01} , then we perform operation X on C to recover it to the information state. If the outcomes are β_{10} and β_{11} , then we take the operation Z and Y respectively.

Here, we show Alice can modify the signature $S_i(j)$ at random as follows: When Alice prepares $|\psi(j)\rangle_M$ and $|a(j)\rangle_{AC}$ in Step (2.1) and Step (2.2), she does not send $|\varphi(j)\rangle_C$ to Charlie and $|\psi(j)\rangle_{MA}$ to U_i immediately. Instead,

she performs a Bell-basis measurement on $|\psi(j)\rangle_{MA}$ to get the outcome β_{kl} and she sends another Bell state $|\beta_{k'l'}\rangle_{MA}$ to U_i . Then the signature $S_i(j) = \beta_{kl}$ has been changed into $S'_i(j) = \beta_{k'l'}$. In order to make sure $S'_i(j)$ can pass the verification, Alice performs a corresponding operator V on $|\varphi(j)\rangle_C$ before sending it to Charlie. Alice can derive the corresponding operator V according to Eq. (14). Assume $|\psi(j)\rangle_M$ is teleported from Alice to Charlie and the measurement outcome is β_{kl} . Also using this equation, Charlie will perform a Pauli operator V_1 on $|\varphi(j)\rangle_C$ to make sure

$$V_1|\varphi(j)\rangle_C \equiv |\psi(j)\rangle_M. \quad (19)$$

In other words, the particle C is in the state

$$|\varphi(j)\rangle_C \equiv V_1|\psi(j)\rangle_M. \quad (20)$$

Here $A \equiv B$ means A is equivalent to B except for a global phase. Alice performs the corresponding V on $|\varphi(j)\rangle_C$, so

$$|\varphi(j)\rangle_C \equiv V^\dagger V_1|\psi(j)\rangle_M. \quad (21)$$

Here V^\dagger is the conjugate transpose of V . When $S_i(j)$ is changed into $S'_i(j)$, Charlie will take another Pauli operator V_2 on $|\varphi(j)\rangle_C$ to return it to the information state $|\psi(j)\rangle_M$, then

$$|\varphi(j)\rangle_C \equiv V_2 V^\dagger V_1 |\psi(j)\rangle_M \equiv |\psi(j)\rangle_M. \quad (22)$$

From Eq. (22), we can conclude that

$$V_2 V^\dagger V_1 = I \quad \text{or} \quad V = V_1 V_2. \quad (23)$$

We take a simple example to make an illustration. Suppose Alice get the measurement outcome β_{00} , but she sends $|\beta_{01}\rangle_{AM}$ to U_i , according to Eq. (14), $V_1 = I$, $V_2 = X$, then $V = X$ according to Eq. (23). We list Alice's attack strategies in Table 1.

3.4 Charlie's attack

In the original scheme, Charlie can also attack the program by modifying the signature S at will.

Charlie is the signature collector whose duty is to collect all the individual signature $S_i (i = 1, 2, \dots, t)$ and extract m'_i by first recovering each $|\varphi(j)\rangle_C$ to $|\psi'(j)\rangle_C$ according to Eq. (14) and then measuring $|\psi'(m)\rangle_C$ in the basis of $\{\frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M)\}$. Charlie can modify the signature S into arbitrary S' and keep the message m'_1 unchanged after confirming the message. Because Bob just verifies whether m is equal to m'_1 or not, S' can pass the verification without being discovered.

$S_i(j) = \beta_{kl} \rightarrow S'_i(j) = \beta_{k'l'}$	V_1	V_2	V
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{01}$	I	X	X
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{10}$	I	Z	Z
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{11}$	I	Y	Y
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{00}$	X	I	X
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{10}$	X	Z	Y
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{11}$	X	Y	Z
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{00}$	Z	I	Z
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{01}$	Z	X	Y
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{11}$	Z	Y	X
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{00}$	Y	I	Y
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{01}$	Y	X	Z
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{10}$	Y	Z	X

Table 1 Alice's attack strategies: First, Alice measures $|\psi(j)\rangle_{MA}$ to get $S_i(j) = \beta_{kl}$, but she sends $|\beta_{k'l'}\rangle_{MA}$ to U_i instead. Then the signature $S_i(j)$ has been changed into $S'_i(j)$. At the same time, Alice performs a corresponding unitary operation V on $|\varphi(j)\rangle_C$ before sending it to Charlie.

3.5 Eavesdropper Eve's forgery attack

In Ref. [51], it is declared that the eavesdropper Eve can't forge U_i 's signature on the assumption that she can get U_i 's secret key K_{CU_i} because of the quantum teleportation. Here we show that Eve can forge U_i 's signature at will even though she knows nothing about the U_i 's key K_{CU_i} .

Here we take a 1-bit message $m(j)$ to make a demonstration. This is an incomplete message $m(j)$ whose signature is $S_i(j)$. Eve replaced $S_i(j)$ with another $S'_i(j)$ when it is sent from U_i to Charlie. Then Charlie will recover the message according to $S'_i(j)$ based on teleportation. Suppose the signature $S_i(j)$ is β_{00} . It is changed into $S'_i(j) = \beta_{01}$ under Eve's attack. We take an illustration as follows:

(1) Without Eve's attack

Suppose the signature $S_i(j)$ is β_{00} and Charlie's particle C is in the state

$$|\varphi(j)\rangle_C = \frac{1}{\sqrt{2}}(|0\rangle_C + d|1\rangle_C), d = \pm 1. \quad (24)$$

Then Charlie will perform I on his particle to recover it to the information state $|\psi'(j)\rangle_C$ according to Eq. (14), here

$$|\psi'(j)\rangle_C = I|\varphi(j)\rangle_C = \frac{1}{\sqrt{2}}(|0\rangle_C + d|1\rangle_C). \quad (25)$$

After that Charlie measures it and extracts the message $m'(j)$ as

$$m'(j) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{if } d = 0. \end{cases} \quad (26)$$

(2) With Eve's attack

The signature is tampered with $S'_i(j) = \beta_{01}$ with Eve's attack, Charlie will perform X on his particle C which is still in the state of Eq. (24). Then the state of C will be

$$|\psi'(j)\rangle_C = X|\varphi(j)\rangle_C = \frac{1}{\sqrt{2}}(|1\rangle_C + d|0\rangle_C). \quad (27)$$

After that, Charlie measures $|\psi'(j)\rangle_C$ to extract the message $m''(j)$ as

$$m''(j) = \begin{cases} 1 & \text{if } d = 1 \\ 0 & \text{if } d = 0. \end{cases} \quad (28)$$

From Eq. (26) and Eq. (28), we can see Charlie will get the same messages, i.e., $m''(j) = m'(j)$. See the list of all the cases in Table 2.

$S_i(j) = \beta_{kl} \rightarrow S'_i(j) = \beta_{k'l'}$	$m''(j)$ and $m'(j)$
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{01}$	$m''(j) = m'(j)$
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{10}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{00} \rightarrow S'_i(j) = \beta_{11}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{00}$	$m''(j) = m'(j)$
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{10}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{01} \rightarrow S'_i(j) = \beta_{11}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{00}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{01}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{10} \rightarrow S'_i(j) = \beta_{11}$	$m''(j) = m'(j)$
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{00}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{01}$	$m''(j) = m'(j) \oplus 1$
$S_i(j) = \beta_{11} \rightarrow S'_i(j) = \beta_{10}$	$m''(j) = m'(j)$

Table 2 The relation between $m'(j)$ and $m''(j)$ under the circumstance that the signature $S_i(j)$ is tampered with by $S'_i(j)$ under Eve's attack.

From the second column of Table 2, we can see β_{00} and β_{01} are interchangeable and so is the β_{10} and β_{11} . Specifically, when Eve tampered with $S_i(j) = \beta_{00}(\beta_{10})$ by $S'_i(j) = \beta_{01}(\beta_{11})$ or vice versa, Charlie will extract the same message. Precisely, $m'(j)$ is equal to $m''(j)$. Accordingly, $S'_i(j)$ can always pass the verification. Eve's other modification of the signature is not interchangeable. We can see all the other cases get different message $m''(j) \neq m'(j)$, but they all satisfy $m''(j) = m'(j) \oplus 1$ where \oplus is modulo 2 addition.

From Table 2, we can make a law of the message and its corresponding signature as follows:

If the signature $S_i(j) = \beta_{kl}$ is changed into $S'_i(j) = \beta_{k'l'}$, then their corresponding messages $m'(j)$ and $m''(j)$ ($k, k', l, l' \in \{0, 1\}$ $j = 1, 2, \dots, n$) will satisfy

$$m''(j) = \begin{cases} m'(j) & \text{if } k = k' \\ m'(j) \oplus 1 & \text{if } k \neq k'. \end{cases} \quad (29)$$

Next we show Eve can forge each signature S_i by the intercept-resend method. Eve can intercept $E_{K_{CU_i}}^C(S_i)$ when it is sent from U_i to Charlie. She adds a $2n$ -bit binary string

$$l = i_1 i_2 \cdots i_{2n} \quad (30)$$

to $E_{K_{CU_i}}^C(S_i)$ and sends it to Charlie. Then Charlie will get

$$S'_i = S_i \oplus l. \quad (31)$$

Charlie will recover the information m'' based on S'_i according to the teleportation rather than S_i . Then Charlie will get

$$m'' = m' \oplus l', \quad (32)$$

where

$$l' = j_1 j_2 \cdots j_n. \quad (33)$$

According to Eq. (29), l' must satisfy

$$j_k = \begin{cases} 0 & \text{if } i_{2k-1} = 0 \\ 1 & \text{if } i_{2k-1} = 1. \end{cases} \quad (34)$$

At the same time, Eve intercepts $E_{K_{AB}}^C(m)$ in the Step (1.3) and resends $E_{K_{AB}}^C(m) \oplus l'$ to Bob. Then Bob will get $m \oplus l'$ instead of m . S'_i will be accepted for the signature of $m \oplus l'$. We can see that Eve's forgery attack can get successful.

4 An improved scheme

Here we present an improved scheme and show it can resist all the attacks mentioned above. Also the secret keys can be reused which can provide efficiency and practicality.

Before we present the improved scheme, it is necessary to introduce the QOTP algorithm it uses. Suppose a quantum message

$$|P\rangle = \bigotimes_{j=1}^n |P_j\rangle \quad (35)$$

is composed of n qubits

$$|P_j\rangle = \alpha_j |0\rangle + \beta_j |1\rangle, \quad (36)$$

where

$$|\alpha_j|^2 + |\beta_j|^2 = 1 \quad (37)$$

and the encryption key $K \in \{0, 1\}^{4n}$. The QOTP encryption E_K used in this scheme on the quantum message can be described as

$$E_K(|P\rangle) = \bigotimes_{j=1}^n \sigma_x^{K_{4j}} \sigma_z^{K_{4j-1}} T \sigma_x^{K_{4j-2}} \sigma_z^{K_{4j-3}} |P_j\rangle \quad (38)$$

where

$$T = \frac{i}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z). \quad (39)$$

This QOTP encryption E_K is the improved one introduced in Ref. [52] for the first time. The assistant operator T can make sure the encrypted message can not be forged in the scheme. Distinctly, for arbitrary message $|P\rangle$, there are no non-identity unitary V and unitary U such that

$$E_K^\dagger V E_K |P\rangle \equiv U |P\rangle. \quad (40)$$

In order to make the secret keys reusable in the improved scheme, we use a one-way hash function here [7]:

$$H(x) : \{0, 1\}^* \longrightarrow \{0, 1\}^{4n}. \quad (41)$$

This scheme also contains four factors: (1) Alice is the message sender. (2) U_i ($i = 1, 2, \dots, t$) is the i -th member of broadcasting multiple signatory. (3) Charlie is the signature collector. (4) Bob is the receiver and the verifier of the broadcasting multiple blind signature.

The improved scheme is also composed of three parts: the initial phase, the individual blind signature generation and verification phase, and the combined multiple blind signature verification phase.

(1) Initial Phase

(1.1) Quantum key distribution

Alice shares the secret key K_{AB} with Bob, K_{AC} with Charlie, and K_{AU_i} ($i = 1, 2, \dots, t$) with each signatory U_i ; Bob shares a secret key K_{BC} with Charlie; Charlie shares secret keys K_{CU_i} ($i = 1, 2, \dots, t$) with each signatory U_i . All the secret keys are $4n$ -bit. To obtain unconditional security, all these keys are distributed via QKD protocols.

(1.2) Message concealing and message transformation

Alice gets $m' = m \oplus r$ where m is an n -bit classical message and r an n -bit random binary string. Alice transforms the classical message m' into n -qubit state

$$|\psi(m')\rangle_M = \bigotimes_{j=1}^n |\psi(j)\rangle_M, \quad (42)$$

where

$$|\psi(j)\rangle_M = \begin{cases} b|0\rangle_M + c|1\rangle_M & \text{if } m'(j) = 1 \\ c|0\rangle_M - b|1\rangle_M & \text{if } m'(j) = 0, \end{cases} \quad (43)$$

b, c are different real constants.

(1.3) Alice sends the message m to Bob

Alice transforms m into $|m\rangle$ as

$$|m\rangle = \bigotimes_{j=1}^n |m(j)\rangle, \quad (44)$$

where

$$|m(j)\rangle = \begin{cases} |0\rangle & \text{if } m(j) = 0 \\ |1\rangle & \text{if } m(j) = 1. \end{cases} \quad (45)$$

Alice randomly chooses a $4n$ -bit binary sequence r_0 , computes $H(K_{AB}||r_0)$, and sends $[E_{H(K_{AB}||r_0)}(|m\rangle)] \otimes |r_0\rangle$ to Bob where

$$|r_0\rangle = \bigotimes_{j=1}^{4n} |r_0(j)\rangle, \quad (46)$$

and

$$|r_0(j)\rangle = \begin{cases} |0\rangle & \text{if } r_0(j) = 0 \\ |1\rangle & \text{if } r_0(j) = 1. \end{cases} \quad (47)$$

Bob extracts r_0 by measuring each particle of $|r_0\rangle$ in the basis $\{|0\rangle, |1\rangle\}$. Then he can compute $H(K_{AB}||r_0)$ and decrypt $E_{H(K_{AB}||r_0)}(|m\rangle)$ to get $|m\rangle$. After that he can get m by performing a measurement in the basis $\{|0\rangle, |1\rangle\}$.

(1.4) Alice sends r to Charlie

$|r\rangle$ is generated as Eq. (46) and Eq. (47). Further more, all the $|r_k\rangle$'s generation in the rest of the scheme is always the same. Alice sends $E_{H(K_{AC}||r_1)}(|r\rangle) \otimes |r_1\rangle$ to Charlie. Then Charlie extracts r by performing a measurement in the computational basis.

(2) The individual blind signature generation and verification phase

In this phase, we pick one of the signatory U_i as the representative who signs the message.

(2.1) Quantum channel setup

Charlie prepares $n+l$ pairs of EPR particles denoted as $\{|a(1)\rangle_{U_iC}, |a(2)\rangle_{U_iC}, \dots, |a(n+l)\rangle_{U_iC}\}$, where $|a(j)\rangle_{U_iC} = \frac{1}{\sqrt{2}}(|00\rangle_{U_iC} + |11\rangle_{U_iC})$, $j = 1, 2, \dots, n+l$. Then he sends the first particle to U_i and keeps the other himself for every EPR pair. After U_i receives all particles, Charlie randomly chooses l particles to perform a measurement randomly in the basis of $\{|0\rangle, |1\rangle\}$ or $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ and reports the position of the particles that he has measured and the basis that he has chosen to U_i . U_i takes the same measurement on the corresponding particles and compares the measurement outcomes with Charlie. If there is no error, the channel is considered to be safe. Otherwise, they abandon the quantum channel and set it up again.

(2.2) Signature Phase

(2.2.1) Alice sends the information quantum state $|\psi(m')\rangle_M$ to U_i

Alice randomly chooses a $4n$ -bit sequence r_2 and computes $H(K_{AU_i}||r_2)$. Then she sends $[E_{H(K_{AU_i}||r_2)}(|\psi(m')\rangle_M)] \otimes |r_2\rangle$ to U_i .

(2.2.2) U_i signs the message m

U_i decrypts $[E_{H(K_{AU_i}||r_2)}(|\psi(m')\rangle_M)]$ to get $|\psi(m')\rangle_M$ by first extracting r_2 and then computing $H(K_{AU_i}||r_2)$. He generates $\{|\psi(j)\rangle_{MU_i} | j = 1, 2, \dots, n\}$ by combining each $|\psi(j)\rangle_M$ with his EPR particle. Then U_i performs a Bell basis measurement on $\{|\psi(j)\rangle_{MU_i} | j = 1, 2, \dots, n\}$ to get the outcomes $\{\beta_{MU_i}(j) | j = 1, 2, \dots, n\}$. According to Eq. (14), $\beta_{MU_i}(j)$ is an Bell state $|\beta_{kl}\rangle$ which can be expressed in 2-bit classical string according to $|\beta_{kl}\rangle \rightarrow kl, k, l \in \{0, 1\}$. By introducing a $4n$ -bit random binary string R_i , U_i gets the blind signature S_i of m' as

$$S_i = (\beta_i \oplus K_{CU_i}) || H[(\beta_i \oplus K_{CU_i}) || R_i] \quad (48)$$

where

$$\beta_i = \beta_{MU_i}(1) || \beta_{MU_i}(2) || \dots || \beta_{MU_i}(j) || \dots || \beta_{MU_i}(n). \quad (49)$$

(2.2.3) U_i sends $|S_i\rangle$ to Charlie

U_i transforms S_i into quantum state $|S_i\rangle$ as

$$|S_i\rangle = \bigotimes_{j=1}^{6n} |S_i(j)\rangle \quad (50)$$

where

$$|S_i(j)\rangle = \begin{cases} |0\rangle & \text{if } S_i(j) = 0 \\ |1\rangle & \text{if } S_i(j) = 1. \end{cases} \quad (51)$$

U_i randomly chooses a 6 dimensional $4n$ -bit string vector $r_3 = (r_3^1, r_3^2, r_3^3, r_3^4, r_3^5, r_3^6)$ and computes $H(K_{CU_i}||r_3)$. Then he sends $[E_{H(K_{CU_i}||r_3)}(|S_i\rangle)] \otimes |r_3\rangle$ to Charlie where

$$H(K_{CU_i}||r_3) = H(K_{CU_i}||r_3^1) || H(K_{CU_i}||r_3^2) || H(K_{CU_i}||r_3^3) || H(K_{CU_i}||r_3^4) || H(K_{CU_i}||r_3^5) || H(K_{CU_i}||r_3^6) \quad (52)$$

and

$$|r_3\rangle = |r_3^1\rangle \otimes |r_3^2\rangle \otimes |r_3^3\rangle \otimes |r_3^4\rangle \otimes |r_3^5\rangle \otimes |r_3^6\rangle. \quad (53)$$

(2.3) Verification Phase

(2.3.1) Charlie decrypts $E_{H(K_{CU_i}||r_3)}(|S_i\rangle)$ to get $|S_i\rangle$, then he can get S'_i by performing a measurement in computational basis. After that he further gets β'_i based on K_{CU_i} according to Eq. (48). Here

$$S'_i = (\beta'_i \oplus K_{CU_i}) || [H[(\beta_i \oplus K_{CU_i}) || R_i]]' \quad (54)$$

If there is no incorrection happened in the transmission and measurement, β'_i and S'_i will be equal to β_i and S_i respectively.

Next, we list the improvements of our new scheme compared to the original one:

- (1) Introducing the improved QOTP encryption algorithm.
- (2) Bringing in a hash function to authenticate the originality of the signature.
- (3) The secret keys become reusable by introducing some random strings.
- (4) Bringing in public boards.
- (5) Classical message is concealed before turning into quantum message. Meanwhile, the transformation method in the improved scheme is according to Eq. (43) rather than Eq. (5) in the original one.
- (6) The entangled quantum channel between Charlie and each $U_i (i = 1, 2, \dots, t)$ is set up by Charlie rather than Alice. At the same time, a channel checking process is added to make sure it is secure.
- (7) Classical message from Alice to Bob is transmitted through quantum method in Step (1.3).

5 Cryptanalysis of the improved scheme

In this section, we present the security analysis of the improved scheme. we show there is no disavowal and forgery in the improved scheme. Meanwhile, we also point out the signatory cannot learn the signed message and the signed message cannot be modified by attackers in the improved scheme.

5.1 No disavowal

5.1.1 Each signatory U_i cannot disavow his signature S_i

From Eq. (48), we can see that because each S_i contains U_i 's secret key K_{CU_i} in the improved scheme, U_i cannot disavow his signature S_i . Meanwhile, U_i cannot disavow S_i by the intercept-resend method mentioned in Ref. [21]. Because in Step (2.3.4) Charlie announces S_i on the public board instead of sending it to Bob, which is only for reading on the public board, U_i can't disavow his signature by intercept-resend method.

5.1.2 The receiver Bob cannot disavow the signature

In the improved scheme, the signature S is announced on the public board by Charlie when Bob informs him $m = m_1^*$ in Step (3.2) so that everyone can witness Bob has received the signature, so Bob can't disavow his receiving the signature. Also, Bob can't disavow the integrity of the signature by claiming $m \neq m_1^*$ as in Ref. [4]. Assume $m = m_1^*$ and Bob lies to claim $m \neq m_1^*$ for his own benefit in Step (3.2). We can ask Alice, Charlie and Bob to public announce the message respectively. Then the dishonest behavior of Bob can be caught according to the voting rule, on the assumption that there is no collaborate attack.

5.2 No forgery

According to Eq. (48), each S_i is composed of β_i , K_{CU_i} and R_i . Here we show there is no participant forgery and external forgery in the improved scheme.

5.2.1 Alice cannot forge the signature

In the improved scheme, Charlie prepares the EPR pairs $\{|a(j)\rangle_{CU_i} |j = 1, 2, \dots, n + l\}$, Alice just prepares the information state $|\psi(m')\rangle_M$ so that she cannot get each β_i by measuring each $|\psi(j)\rangle_{MU_i}$ directly. Next we show Alice cannot get β_i by intercept-resend method either. Assume Alice intercepts each $|\varphi(j)\rangle_{U_i}$ and resends the measurement outcome $|\beta_{kl}\rangle_{MU_i}$ to U_i . Because Charlie and U_i performs a checking process in Step (2.1), Alice's intercept-resend attack will be discovered. According to the improved scheme, Alice cannot get β_i . K_{CU_i} is shared between Charlie and U_i via QKD protocol so that Alice has no chance to get it. Moreover, R_i is chosen by U_i randomly and it is not acquired by anyone else until it is announced on the public board so that Alice cannot get it in the signing phase. Therefore, Alice cannot forge the signature.

5.2.2 Charlie cannot forge the signature

Charlie, the signature collector who can get each S'_i and the secret key K_{CU_i} in the improved scheme, is considered to be most likely to forge the signature successfully. Here we show he cannot forge the signature either. Charlie can modify the signature at random and keep the message unchanged when he has confirmed the message, which has no influence on the following message comparison. Charlie cannot learn each U_i 's random string R_i . Since he does not know how to modify $H'[(\beta_i \oplus K_{CU_i})||R_i]$ to fit his modification deterministically, Charlie's forgery attack can definitely be discovered in Step (3.2).

5.2.3 Bob cannot forge the signature

Bob is the receiver of the scheme, he cannot get the signature S until Charlie announced it on the public board. Therefore, the only way Bob can modify the signature is to perform a unitary operator V on $E_{H(K_{CU_i}||r_3)}(|S_i\rangle)$ in Step (2.2.3). According to Eq. (40), Bob's modification cannot follow his will, then it will be definitely discovered in the verification process. As a consequence, Bob cannot forge the signature.

5.2.4 The eavesdropper Eve cannot forge the signature

In the improved scheme, the classical bit $m'(j)$ is transformed into quantum state according to Eq. (42) and Eq. (43). Here we take a 1-bit message $m'(j)$ to illustrate any of Eve's modification on $S_i(j)$ can be detected.

Supposed $S_i(j) = \beta_{01}$ is replaced with $S'_i(j) = \beta_{00}$ by Eve, the corresponding message are $m'(j)$ and $m''(j)$ respectively. We present this case as follows:

(1) Without Eve's attack:

(1.1) Assume Alice prepares the state $|\psi(j)\rangle_M = b|0\rangle_M + c|1\rangle_M$ and its signature is $S_i(j) = \beta_{01}$, according to the teleportation, Charlie's particle will be in the state $|\varphi(j)\rangle_C = b|1\rangle_C + c|0\rangle_C$. Then Charlie performs operation X on $|\varphi(j)\rangle_C$ to get the state $|\psi'(j)\rangle_C = b|0\rangle_C + c|1\rangle_C$. After that Charlie performs a measurement in the basis of $\{b|0\rangle_M + c|1\rangle_M, c|0\rangle_M - b|1\rangle_M\}$ to extract $m'(j) = 1$.

(1.2) Assume Alice prepares the state $|\psi(j)\rangle_M = (c|0\rangle_M - b|1\rangle_M)$ and its signature is $S_i(j) = \beta_{01}$, according to the teleportation, Charlie's particle will be in the state $|\varphi(j)\rangle_C = c|1\rangle_C - b|0\rangle_C$. Then Charlie performs operation X on $|\varphi(j)\rangle_C$ to get the state $|\psi'(j)\rangle_C = c|0\rangle_C - b|1\rangle_C$. After that Charlie performs a measurement in the basis of $\{b|0\rangle_M + c|1\rangle_M, c|0\rangle_M - b|1\rangle_M\}$ to extract $m'(j) = 0$.

(2) With Eve's attack:

(2.1) Assume Alice prepares the state $|\psi(j)\rangle_M = b|0\rangle_M + c|1\rangle_M$ and Eve replaces $S_i(j) = \beta_{01}$ with $S'_i(j) = \beta_{00}$, then Charlie's particle is still in the state $|\varphi(j)\rangle_C = b|1\rangle_C + c|0\rangle_C$ as Eve's attack has no effect on it. According to the teleportation, Charlie will perform operation I on $|\varphi(j)\rangle_C$ to get $|\psi'(j)\rangle_C = b|1\rangle_C + c|0\rangle_C$. After that Charlie performs a measurement in the basis of $\{b|0\rangle_M + c|1\rangle_M, c|0\rangle_M - b|1\rangle_M\}$ to extract $m''(j)$, it will have a probability of $4b^2c^2$ to get $m''(j) = 1$ and a probability of $c^4 + b^4 - 2b^2c^2$ to get $m''(j) = 0$.

(2.2) Assume Alice prepares the state $|\psi(j)\rangle_M = (c|0\rangle_M - b|1\rangle_M)$ and Eve replaces $S_i(j) = \beta_{01}$ with $S'_i(j) = \beta_{00}$, then Charlie's particle is still in the state $|\varphi(j)\rangle_C = c|1\rangle_C - b|0\rangle_C$. According to the teleportation, Charlie will perform operation I on $|\varphi(j)\rangle_C$ to get $|\psi'(j)\rangle_C = c|1\rangle_C - b|0\rangle_C$. After that Charlie performs a measurement in the basis of $\{b|0\rangle_M + c|1\rangle_M, c|0\rangle_M - b|1\rangle_M\}$ to extract $m''(j)$, it will have a probability of $c^4 + b^4 - 2b^2c^2$ to get $m''(j) = 1$ and a probability of $4b^2c^2$ to get $m''(j) = 0$.

From (1) and (2), we can see that Eve's modification of the signature can be discovered in Step (2.3.4) with a non-zero probability. Other cases can be presented similarly. We can see Eve cannot forge the signature.

5.3 Each U_i cannot learn the signed message

In the improved scheme, the classical message m is turned into $m' = m \oplus r$ before it is transformed into quantum states. If U_i performs a measurement in the basis of $\{b|0\rangle_M + c|1\rangle_M, c|0\rangle_M - b|1\rangle_M\}$ on the information quantum sequence $\{|\psi(j)\rangle_M | j = 1, 2, \dots, n\}$, he will just get m' and has no chance to get the signed message m . If he wants to learn m , he has to know r which will be sent from Alice to Charlie in Step (1.4). Because r is turned into $|r\rangle$ and encrypted by K_{AC} according to the quantum one-time pad algorithm during

its transmission, U_i cannot get the random string r without the key K_{AC} . Therefore, we know U_i can't learn the signed message m .

5.4 The signed message m cannot be modified

In the improved scheme, the signed message m is turned into quantum state $|m\rangle$ according to Eq. (44) and Eq. (45) before it is sent from Alice to Bob in Step (1.3). It is encrypted by $H(K_{AB}||r_0)$ according to Eq. (38). Here we show any attacker without the key K_{AB} cannot modified the message m by the intercept-resend method. Suppose the attacker wants to modify the signed message m . He intercepts the $[E_{H(K_{AB}||r_0)}(|m\rangle)] \otimes |r_0\rangle$. Because he does not get the secret key K_{AB} , the attacker cannot decrypt it directly. Then he can choose to perform a unitary operator V on $[E_{H(K_{AB}||r_0)}(|m\rangle)]$ and send $V[E_{H(K_{AB}||r_0)}(|m\rangle)] \otimes |r_0\rangle$ to Bob. In order to make sure this modification can pass the verification, there must exist a non-identity unitary operator U to satisfy Eq. (40). Because $|m\rangle$ is from classical message m according to Eq. (44) and Eq. (45), here U can be restricted to Pauli operators. Exactly

$$\begin{aligned} V[E_{H(K_{AB}||r_0)}(|m\rangle)] &\equiv E_{H(K_{AB}||r_0)}(U|m\rangle) \\ U &= \bigotimes_{j=1}^n Q_j \\ Q_j &\in \{I, \sigma_x, \sigma_y, \sigma_z\} \end{aligned} \quad (57)$$

The question the attacker has to face now is whether there exist such non-identity unitary operators U and V to satisfy Eq. (57). Unfortunately, it is pointed out that there doesn't exist such U and V for any message $|m\rangle$ in Ref. [52]. Then the modification mentioned above will be discovered in the verification process.

Next, we show Bob can modify the signed message m at random in the improved scheme, but we can rebut it by the voting rule when this dispute takes place. Because Bob has got K_{AB} and K_{BC} , according to the improved scheme, he can modify m at random and make this modification can pass the verification. When the dispute on the message m happens between Alice and Bob, we can ask Alice, Bob and Charlie to public their message and arbitrate it according to the voting rule on the assumption that they are all just loyal to themselves. From above, we can see the signed message cannot be modified in the improved scheme.

6 Conclusion.

In this paper, we first gave a security analysis on the quantum broadcasting multiple blind signature scheme based on teleportation in Ref. [51], which has recently been proposed. We point out that there are some security loopholes in the protocol and describe the attack strategies in detail. Then we present an

improved scheme by introducing hash function, public board, and the improved QOTP encryption algorithm proposed in Ref. [52]. After that, we show the improved scheme can resist all the mentioned attacks and that the secret keys can be reusable by bringing in some random strings. The improved scheme is more practical and secure. It will have foreseeable applications to E-payment system, E-business, and E-government.

The improved quantum broadcasting multiple blind signature can only sign classical message. So it is worthwhile for us to designing a scheme for quantum messages in the future.

References

1. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* 26(5), 1484-1509 (1997)
2. Zeng G, Keitel C H.: Arbitrated quantum-signature scheme. *Phys. Rev. A.* 65(4), 042312 (2002)
3. Li, Q, Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. *Phys. Rev. A.* 79(5), 054307 (2009)
4. Zou X, Qiu D.: Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A.* 82(4), 042325 (2010)
5. Li Q, Li C, Long D, et al.: Efficient arbitrated quantum signature and its proof of security. *Quantum Inf. Process.* 12(7), 2427-2439 (2013)
6. Luo Y P, Hwang T.: Arbitrated quantum signature of classical messages without using authenticated classical channels. *Quantum Inf. Process.* 13(1), 113-120 (2014)
7. Yu C.H, Guo G.D, Lin S.: Arbitrated quantum signature scheme based on reusable key. *Sci. Ch. Phys. Mech. Astron.* 57(11), 2079-2085 (2014)
8. Yin X R, Ma W P, Liu W Y.: Quantum proxy group signature scheme with -type entangled states. *Int. J. Quantum Inform.* 10, 1250041 (2012)
9. Wang T Y, Wei Z L.: One-time proxy signature based on quantum cryptography. *Quantum Inf. Process.* 11(2), 455-463 (2012)
10. Wen X, Chen Y, Fang J.: An inter-bank E-payment protocol based on quantum proxy blind signature. *Quantum Inf. Process.* 12(1), 549-558 (2013)
11. Cao H J, Huang J, Yu Y F, et al.: A Quantum Proxy Signature Scheme Based on Genuine Five-qubit Entangled State. *Int. J. Theor. Phys.* 53(9), 3095-3100 (2014)
12. Wen X, Tian Y, Ji L, et al.: A group signature scheme based on quantum teleportation. *Phys. Scr.* 81(5), 055001 (2010)
13. Xiaojun W. :An E-payment system based on quantum group signature. *Phys. Scr.* 82(6), 065403 (2010)
14. Xu R, Huang L, Yang W, et al.: Quantum group blind signature scheme without entanglement. *Opt. Commun.* 284(14), 3654-3658 (2011)
15. Zhang K, Song T, Zuo H, et al.: A secure quantum group signature scheme based on Bell states. *Phys. Scr.* 87(4), 045012 (2013)
16. Qi S, Zheng H, Qiaoyan W, et al.: Quantum blind signature based on two-state vector formalism. *Opt. Commun.* 283(21), 4408-4410 (2010)
17. Yin X R, Ma W P, Liu W Y. :A blind quantum signature scheme with -type entangled states. *Int. J. Theor. Phys.* 51(2), 455-461 (2012)
18. Lin T S, Chen Y, Chang T H, et al.: Quantum blind signature based on quantum circuit. *Nanotechnology (IEEE-NANO)*, 2014 IEEE 14th International Conference on. IEEE, 868-872 (2014)
19. Wen X J, Liu Y, Sun Y.: Quantum multi-signature protocol based on teleportation. *Zeitschrift fur Naturforschung A.* 62(3/4), 147 (2007)
20. Wen X, Liu Y.: A realizable quantum sequential multi-signature scheme. *Dianzi Xuebao(Acta Electronica Sinica).* 35(6), 1079-1083 (2007)
21. Gao F, Qin S J, Guo F Z, et al.: Cryptanalysis of the arbitrated quantum signature protocols. *Phys. Rev. A.* 84(2), 022344 (2011)

22. Choi J W, Chang K Y, Hong D.: Security problem on arbitrated quantum signature schemes. *Phys. Rev. A* 84(6), 062330 (2011)
23. Zuo H, Zhang K, Song T.: Security analysis of quantum multi-signature protocol based on teleportation. *Quantum Inf. Process.* 12(7), 2343-2353 (2013)
24. Kejia Z, Dan L, Qi S.: Security of the arbitrated quantum signature protocols revisited. *Phys. Scr.* 89(1), 015102 (2014)
25. Yang C W, Luo Y P, Hwang T.: Forgery attack on one-time proxy signature and the improvement. *Quantum Inf. Process.* 13(9), 2007-2016 (2014)
26. Liu Z H, Chen H W, Wang D, et al.: Cryptanalysis and improvement of three-particle deterministic secure and high bit-rate direct quantum communication protocol. *Quantum Inf. Process.* 13(6), 1345-1351 (2014)
27. Wang T Y, Cai X Q, Zhang R L.: Security of a sessional blind signature based on quantum cryptograph. *Quantum Inf. Process.* 13(8), 1677-1685 (2014)
28. Lo, H., Ko, T.: Some attacks on quantum-based cryptographic protocols. *Quantum Inf. Comput.* 5(1), 41-48 (2005)
29. Gao, F., Guo, F., Wen, Q., Zhu, F.: Comment on Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection. *Phys. Rev. Lett.* 101, 208901 (2008)
30. Zhang, Y., Li, C., Guo, G.: Comment on Quantum key distribution without alternative measurements [Phys. Rev. A 61, 052312 (2000)]. *Phys. Rev. A* 63, 036301 (2001)
31. Gao, F., Qin, S., Wen, Q., Zhu, F.: A simple participant attack on the Bradler-Dusek protocol. *Quantum Inf. Comput.* 7(4), 329-334 (2007)
32. Wang, T., Wen, Q., Chen, X.: Cryptanalysis and improvement of a multi-user quantum key distribution protocol. *Opt. Commun.* 283(24), 5261-5263 (2010)
33. Gao, F., Wen, Q., Zhu, F.: Teleportation attack on the QSDC protocol with a random basis and order. *Chin. Phys. B* 17(9), 3189 (2008)
34. Wang, T., Wen, Q., Gao, F., et al.: Cryptanalysis and improvement of multiparty quantum secret sharing schemes. *Phys. Lett. A* 373(1), 65-68 (2008)
35. Gao, F., Qin, S., Guo, F., Wen, Q.: Dense-coding attack on three-party quantum key distribution protocols. *IEEE J. Quant. Electron.* 47(5), 630-635 (2011)
36. Hao, L., Li, J., Long, G.: Eavesdropping in a quantum secret sharing protocol based on Grover algorithm and its solution. *Sci. Chin. Phys. Mech. Astron.* 53(3), 491-495 (2010)
37. Qin, S., Gao, F., Wen, Q., Zhu, F.: Improving the security of multiparty quantum secret sharing against an attack with a fake signal. *Phys. Lett. A* 357(2), 101-103 (2006)
38. Wójcik, A.: Eavesdropping on the Ping-Pong quantum communication protocol. *Phys. Rev. Lett.* 90, 157901 (2003)
39. Wójcik, A.: Comment on Quantum dense key distribution. *Phys. Rev. A* 71, 016301 (2005)
40. Cai, Q.: The Ping-Pong protocol can be attacked without eavesdropping. *Phys. Rev. Lett.* 91, 109801 (2003)
41. Gao, F., Guo, F., Wen, Q., Hu, F.: Consistency of shared reference frames should be reexamined. *Phys. Rev. A* 77, 014302 (2008)
42. Gao, F., Wen, Q., Zhu, F.: Comment on: Quantum exam [Phys. Lett. A 350 (2006) 174]. *Phys. Lett. A* 360(6), 748-750 (2007)
43. Gao, F., Lin, S., Wen, Q., Zhu, F.: A special eavesdropping on one-sender versus N-receiver QSDC protocol. *Chin. Phys. Lett.* 25(5), 1561 (2008)
44. Gao, F., Qin, S., Wen, Q., Zhu, F.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Opt. Commun.* 283(1), 192-195 (2010)
45. Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* 73, 022320 (2006)
46. Deng, F., Li, X., Zhou, H., Zhang, Z.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* 72, 044302 (2005)
47. Jain N, Anisimova E, Khan I, et al.: Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* 16(12), 123030 (2014)
48. Yang Y G, Sun S J, Zhao Q Q.: Trojan-horse attacks on quantum key distribution with classical Bob. *Quantum Inf. Process.* 14(2), 681-686 (2014)
49. Wang, T., Wen, Q.: Security of a kind of quantum secret sharing with single photons. *Quantum Inf. Comput.* 11(5), 434-443 (2011)

-
50. Wang, T., Wen, Q., Zhu, F.: Cryptanalysis of multiparty quantum secret sharing with Bell states and Bell measurements. *Opt. Commun.* 284(6), 1711-1713 (2011)
 51. Tian Y, Chen H, Ji S, et al.: A broadcasting multiple blind signature scheme based on quantum teleportation. *Opt. Quan. Elec.* 46(6), 769-777 (2014)
 52. Kim T, Choi J W, Jho N S, et al.: Quantum messages with signatures forgeable in arbitrated quantum signature schemes. *Phys. Scr.* 90(2), 025101 (2015)